Experiment No: 09

Experiment Name: Network Address Translation (NAT) Configuration.

Theory:

Network Address Translation (NAT) allows devices in private networks to communicate with external public networks by translating private IP addresses to public IP addresses. NAT helps conserve IPv4 addresses and provides controlled access between private and public networks.

In NAT configuration, router interfaces are classified as inside (private) or outside (public), which determines how traffic is translated. NAT supports **two** main types:

- **Static NAT:** Maps a private IP to a public IP permanently, allowing external users to access internal servers (e.g., web servers).
- **Port Address Translation (PAT) / NAT Overload:** Allows multiple private hosts to share a single public IP, using unique source ports for each session. This is commonly used for outbound client traffic.

Components:

1. Cisco Packet Tracer
2. PT-Routers
3. PT-Switches
4. Web Servers
5. PCS/Laptops
6. Connection Cables

Procedures:

Task 1: Static NAT Configuration (2 Routers, 2 Switches, 4 PCs, 1 Web Server)

Objective: To configure Router 2 to use Static NAT to allow inbound web access to the internal server (172.16.5.2) and NAT Overload (PAT) to allow all internal clients (172.16.5.0/24) to access the outside network (192.168.10.0/24).

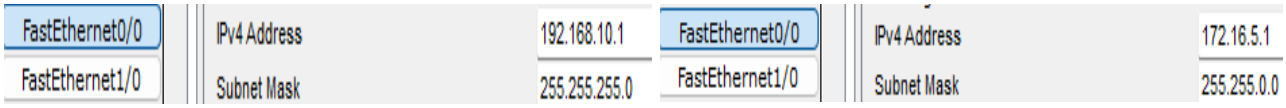

Figure 01: Fast-Ethernet Configuration.

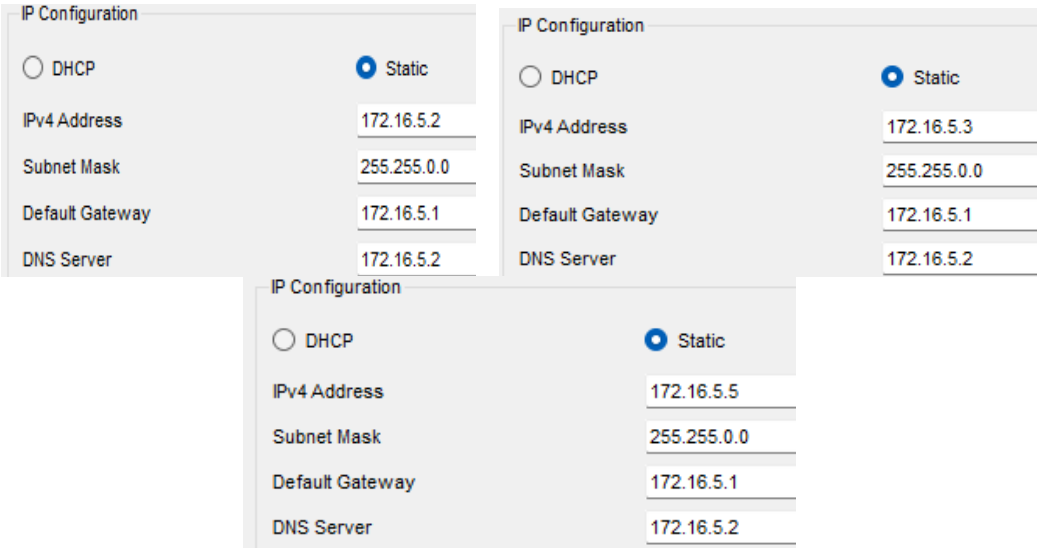

Figure 02: Static IP Configuration.

Device	Interface	IP Address / Configuration	Gateway
Router-PT (R2)	Fa0/0 (Inside)	172.16.5.1 (255.255.0.0)	—
Router-PT (R2)	Se2/0 (Outside)	192.168.20.2 (255.255.255.0)	—
Web Server	Fa0	172.16.5.2 (Static)	172.16.5.1
Laptop-PT (Client)	Fa0	172.16.5.5 (Static)	172.16.5.1
Router-PT (R1)	Fa0/0	192.168.10.1 (255.255.255.0)	—

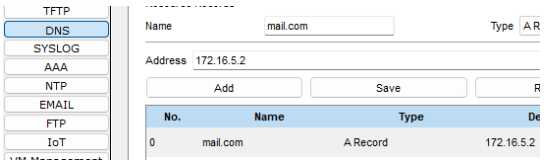

Figure 03: DNS Add.

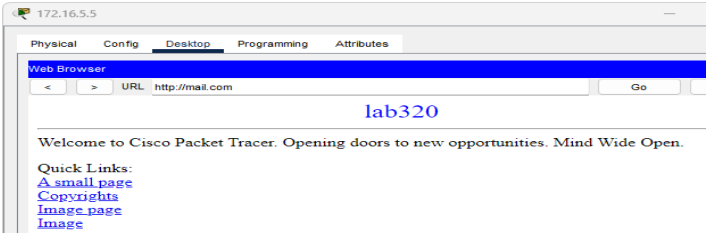

Figure: 04 Web Browser Check.

Configuration Steps:

1. Configure Router Interfaces (R2 - NAT Router):
   - Set IP addresses and define NAT boundaries (inside or outside).

Router> en
Router# conf t
Router(config)# int fa0/0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# int se2/0
Router(config-if)# ip nat outside
Router(config-if)# exit

2. Configure Static NAT for router 2:
   - Router(config)# ip nat inside source static 172.16.5.2 192.168.20.2
   - Router(config)# ip nat inside source static 172.16.5.3 192.168.20.2
   - Router(config)# ip nat inside source static 172.16.5.5 192.168.20.2

```
Router(config)#ip nat inside source static 172.16.5.2 192.168.20.2
Router(config)#ip nat inside source static 172.16.5.3 192.168.20.2
Router(config)#ip nat inside source static 172.16.5.5 192.168.20.2
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int se2/0
Router(config-if)#ip nat outside
```

Figure 05: NAT Configuration.

3. Configure NAT Overload (PAT) for Clients:
   - R2 Route: Add a static route on R2
   - Router(config)# ip route 192.168.10.0 255.255.255.0 192.168.20.1

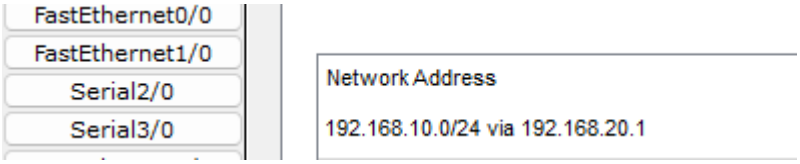

Figure 06: Static Routing Configuration.

4. Verification:
   - Verify NAT translations after testing connectivity (inbound access to 192.168.20.2 and outbound access from 172.16.5.0 to 192.168.10.0).

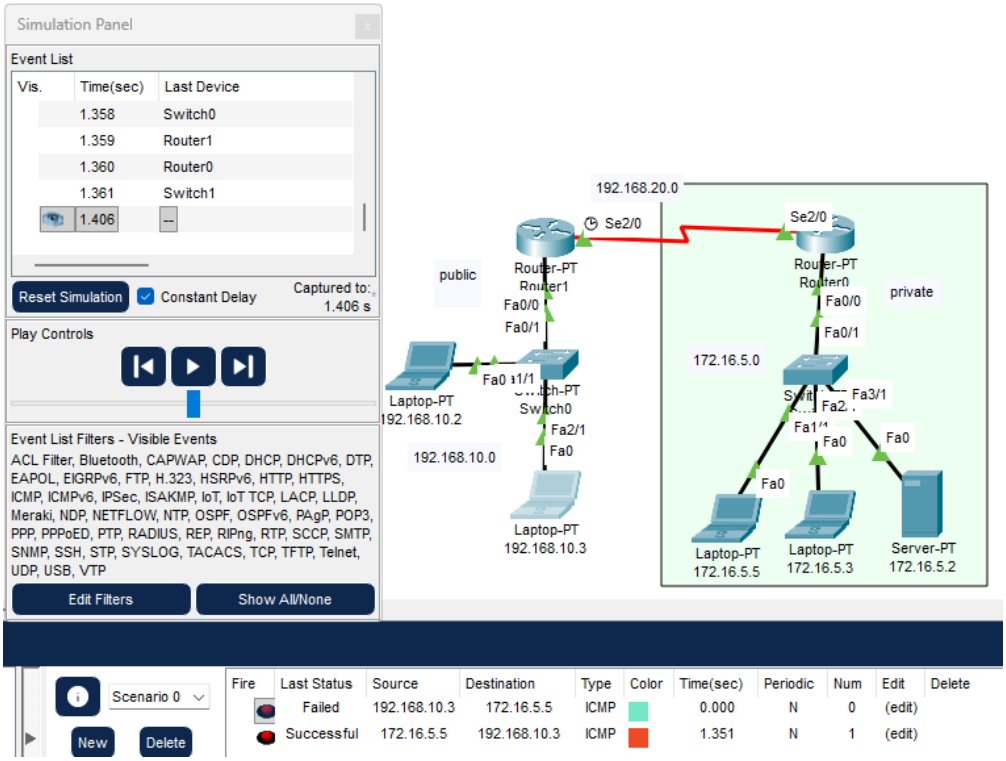

Figure 07: Static NAT Configuration.

Task 2: Advanced NAT Configuration (3 Routers, 3 Switches, 7 PCs, 2 Servers)

Objective: To configure a transit network involving three routers (R1, R2, R3) for multiple NAT scenarios. R1 handles NAT for 192.168.30.0/24 and R3 handles NAT for 172.16.5.0/24. R2 acts as a central transit router, requiring robust static routing to ensure all networks are reachable.

Device	Interface	IP Address
R1 (Left NAT Router)	Fa0/0	192.168.30.1
R1 (Left NAT Router)	Se2/0	192.168.40.1
R2 (Transit Router)	Se2/0	192.168.20.1
R2 (Transit Router)	Se3/0	192.168.40.2
R3 (Right NAT Router)	Se2/0	192.168.20.2
R3 (Right NAT Router)	Fa0/0	172.16.5.1
Server 1	Fa0	192.168.30.5
Server 2	Fa0	172.16.5.2

Configuration Steps:

1. Configure Interface IPs and NAT Boundaries:

   Configure Static NAT for Both Servers:

   - On R1: Web Server 1 (192.168.30.5) to R1's public IP (192.168.40.1).
   - On R3: Web Server 2 (172.16.5.2) to R3's public IP (192.168.20.2).

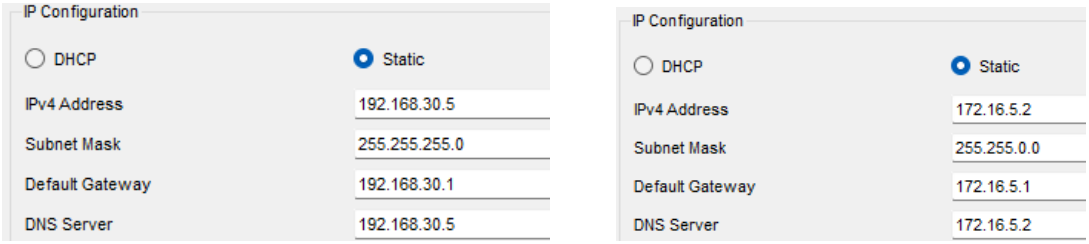

Figure 08: Web Server IP Configuration.

2. CLI input in Router3 for NAT configuration:
   - Router3(config)# ip nat inside source static 172.16.5.2 192.168.20.2
   - Router3(config)# ip nat inside source static 172.16.5.3 192.168.20.2
   - Router3(config)# ip nat inside source static 172.16.5.5 192.168.20.2

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside  source static 172.16.5.2 192.168.20.2
Router(config)#ip nat inside  source static 172.16.5.3 192.168.20.2
Router(config)#ip nat inside  source static 172.16.5.5 192.168.20.2
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int se2/0
Router(config-if)#ip nat outside
```

Figure 09: NAT Configuration Using CLI.

3. Configure Static Routing (All Routers):
   - Router1(config)# ip route 192.168.10.0 255.255.255.0 192.168.40.2
   - Router3(config)# ip route 192.168.30.0 255.255.255.0 192.168.20.1
   - Router3(config)# ip route 192.168.30.0 255.255.255.0 192.168.40.2
   - Router2(config)# ip route 192.168.30.0 255.255.255.0 192.168.40.1

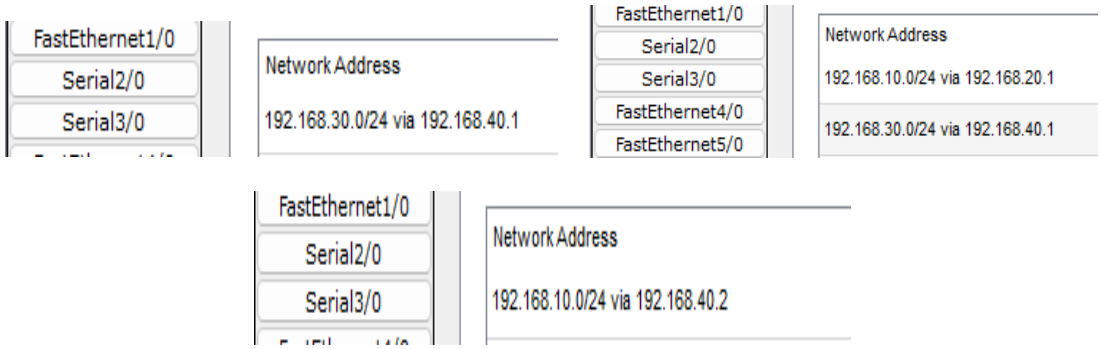

Figure 10: Static Configuration.

4. RIP in All routers.

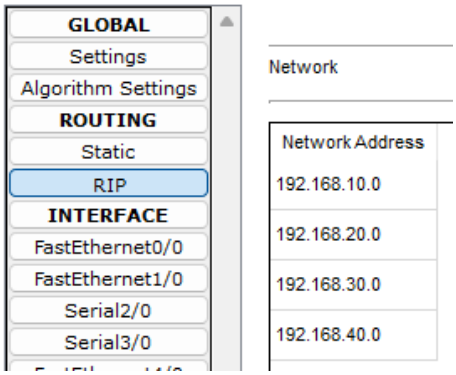

Figure 11: RIP Configuration.

5. Verification:
   - Test cross-network communication (e.g., a client on 172.16.5.0 accesses Server 1 on 192.168.30.0) and verify the resulting NAT entries on both R1 and R3.

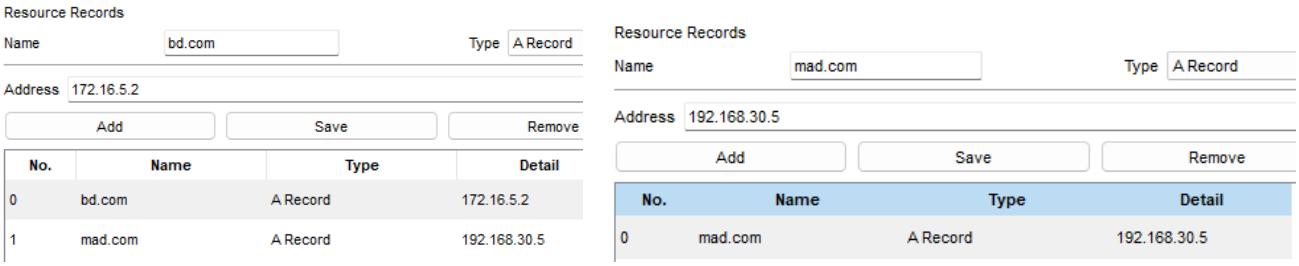

Figure 12: DNS Configuration.

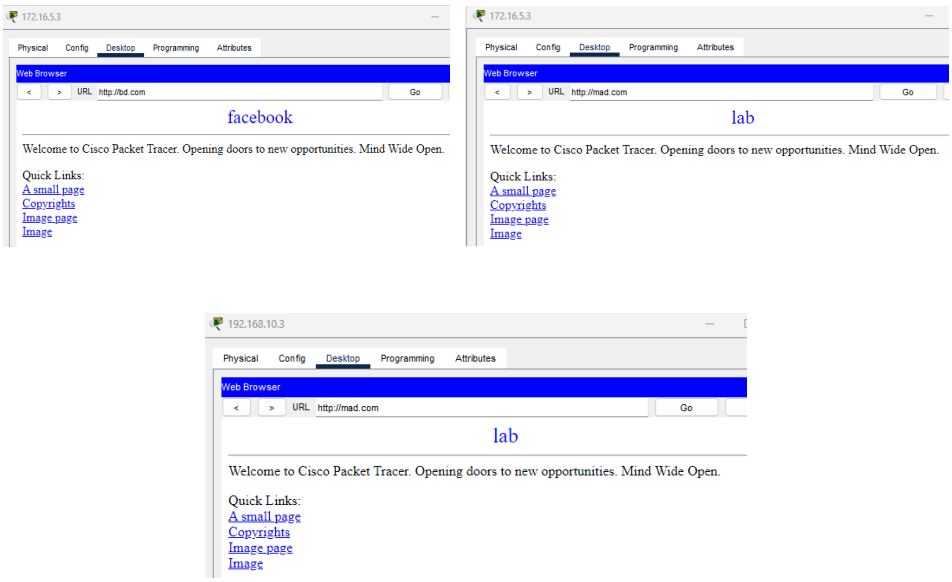

Figure 13: Web page Check.

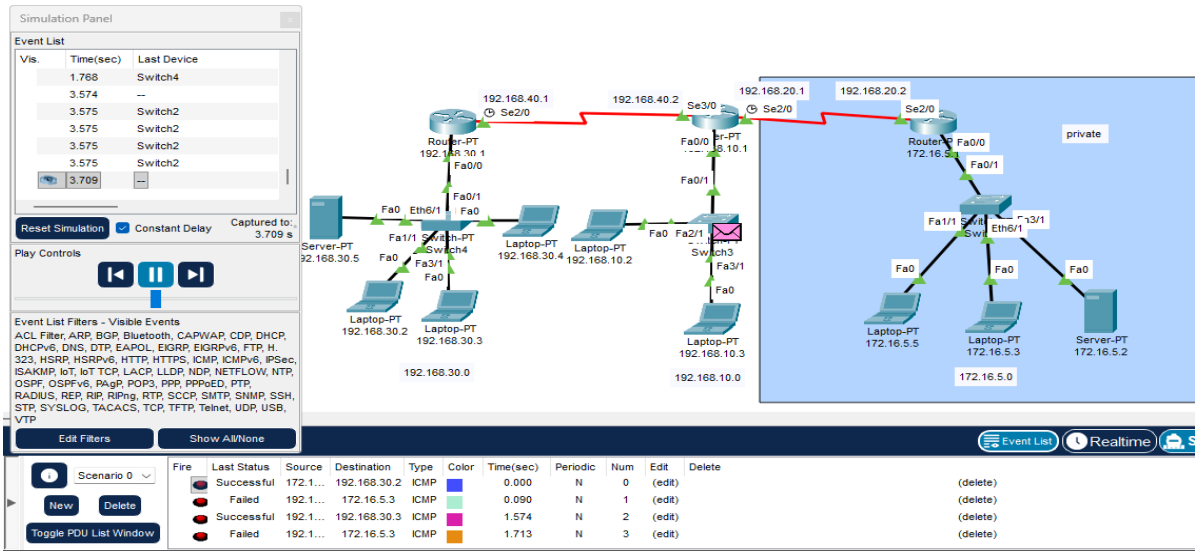

Figure 14: Advanced NAT Configuration.

Conclusion:

This experiment showed how NAT controls communication between private and public networks. Private hosts can access public networks because NAT creates temporary translation entries. However, public hosts cannot access private devices unless Static NAT (port forwarding) is configured. Task 1 demonstrated outbound access using PAT and inbound access using Static NAT. Task 2 confirmed the same behavior across multiple routers, highlighting that correct routing is required for NAT-translated traffic to reach its destination.